NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 1600.1
Effective Date:
November 03, 2004
Expiration Date:
November 03, 2014

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Security Program Procedural Requirements w/Change 2 (4/01/2009)

Responsible Office: Office of Protective Services

Chapter 5. Classified National Security and Sensitive but Unclassified (SBU) Information Management

5.1 General

5.1.1. NASA generates, receives, disseminates, and maintains an enormous amount of information, much of which is of an unclassified/nonsensitive nature with few restrictions on its use and dissemination.

5.1.2. NASA also generates, receives, stores, disseminates, and maintains classified national security information (CNSI) under a variety of Agency programs, projects, and through partnerships and collaboration with other federal agencies, academia, and private enterprises.

5.1.3. In accordance with EO 12958, "Classified National Security Information," as amended, this chapter establishes Agency procedures for the proper implementation and management of a uniform system for classifying, accounting, safeguarding, and declassifying national security information generated by or in the possession of NASA.

5.1.4. Nothing in this chapter or the applicable EO limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act of 1974, and the National Security Act of 1947.

5.1.5. This chapter also establishes a uniform process whereby sensitive but unclassified (SBU) NASA information, known as "Administratively Controlled Information (ACI)," is identified and properly managed to ensure disclosure to unauthorized persons is effectively prohibited.

5.1.6. Further, this chapter defines the security review requirements for programs and projects, pursuant to NPR 7120.5 series, and establishes procedures for the creation of Security Classification Guides (SCG), as well as requirements for reviewing permanent historical documents, pursuant to NPR 1441.1 series, for continued classification before retirement into Federal Records Centers (FRC) or the National Archives and Records Administration (NARA).

5.2 Responsibilities

5.2.1. Per ISOO Directive 1, Section 2001.61(b)(6)(iii)(E), the Administrator will ensure that individual performance plans will include management of classified information as a critical element for "cleared" personnel whose duties "significantly involve the creation or handling of classified information." In this context, "significant involvement" means at least 50% of duty time is involved in activity related to accessing, creating, or handling CNSI.

5.2.2. The AA/OSPP is responsible for providing direction and oversight for an Agency-wide administrative security program and implementation of EO 12958 for the protection of CNSI and SBU in NASA's custody. He/she shall:

5.2.2.1. Establish Agency-wide procedures pertaining to the management of CNSI and material, and ACI generated by or in the custody of NASA.

5.2.2.2. Periodically review Center procedures and systems to ensure CNSI and ACI are properly protected against unauthorized disclosure or access.

5.2.3. Center Directors are responsible, through the CCS, for ensuring proper planning and implementation of EO 12958, and managing classified information and material and ACI under the jurisdiction and custody of their respective Centers. This responsibility includes component activities geographically separated from the parent Center.

5.2.4. The CCS shall ensure an information security program for CNSI is developed, implemented, and maintained at a level sufficient to meet the requirements of this chapter and national level requirements. This includes:

5.2.4.1. Developing and implementing appropriate processes and procedures for classifying NASA information per EO 12958 and other national level requirements.

5.2.4.2. Developing and implementing appropriate processes and procedures for automatic declassification per EO 12958.

5.2.4.3. Developing and implementing procedures for the appropriate safeguarding of CNSI and ACI.

5.2.4.4. Conducting periodic reviews of NASA organizational units involved in classified work and storage of classified material to ensure compliance with EO 12958, this NPR, and any applicable local procedures. Reviews shall be conducted in a manner that meets the intent of ISOO Directive No.1, Subpart C, and shall be reported in Block 9 of Standard Form 311, Agency Security Classification Management Program.

5.2.4.5. Promptly and fully determining the circumstances surrounding any loss or possible compromise of classified information or material and initiating appropriate investigative action.

5.2.4.6. Establishing more stringent standards, specifications, procedures, or guidelines when special conditions or circumstances arise that indicate increased safeguards are necessary in the interest of national security.

5.2.5. NASA supervisors at all levels shall ensure that all personnel entrusted with classified information or material are fully knowledgeable of and comply with the provisions set forth in this NPR and established National level policies governing accessing, protecting, accounting for, and safeguarding classified information and material, and that management of classified information be included in individual performance plans as a critical element .

5.2.6. Employees entrusted with CNSI shall immediately report the following to the CCS:

5.2.6.1. Loss or suspected compromise of classified information or material.

5.2.6.2. Known or suspected practice or condition that compromises the proper safeguarding and handling of classified information or material.

5.2.6.3. Attempts by uncleared personnel, or personnel with no need-to-know, to gain access to CNSI.

5.2.6.4. Initial classification, downgrading, or declassification actions associated with NASA generated information or material.

5.2.7. All personnel entrusted with CNSI are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. This will be accomplished by:

a. Submit in writing, to the CCS, the justification for the challenge.

b. Ensure the written challenge carries the same classification level as the original. Control as classified information.

c. The CCS will review and, where necessary, consult the original classification authority, to assist in determining the merits of the challenge, and:

(1). Grant the challenge and adjust the classification level as appropriate, or;

(2). Deny the challenge, provide rational for the denial, as appropriate, or;

(3). Refer the challenge the challenge to the NASA Information Security Program Committee who will make the final Agency determination, or;

(4). The NASA Information Security Program Committee may refer the challenge to the Information Security Oversight Office (ISOO) for final determination.

5.3 Agency Information Security Program Data Report, SF-311

Annual SF-311 reports are required at the end of each fiscal year. The reporting period is from October 1 to September 30. The CCS shall submit an unclassified report to the Director, NASA Security Management Office, no later than October 15 following the reporting period.

5.4 Classifying, Marking, and Declassifying CNSI

5.4.1. Classification. Information is classified pursuant to EO 12958 by an Original Classification Authority and is designated and marked as Top Secret, Secret, or Confidential. Except as provided by statute, no other terms may be used to identify classified information.

5.4.1.1. Classification challenges. Authorized holders of classified information wishing to challenge the classification status of information shall present such challenges, per subparagraph 5.2.7, to the Director, Security Management Division (DSMD), Office of Security and Program Protection (OSPP). Once the challenge is received, a determination will be made to submit the challenge to an original classification authority with jurisdiction over the information. A formal challenge under this provision must be in writing, but need not be any more specific than to question why information is or is not classified, or is classified at a certain level. An attempt shall be made to keep all challenges, appeals and responses unclassified. However, if it's necessary to include classified information into a challenge, please contact your local Security Office to assist you with preparing the classified challenge. The following procedures will be followed when processing a challenge:

a. The DSMD shall provide an initial written response to a challenge within 60 days.

b. If the DSMD is unable to respond in 60 days, the challenge will be acknowledge in writing and the letter will include a response date.

c. The challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel (ISCAP) for a decision.

d. The challenger may also forward the challenge to the ISCAP if an agency has not responded to an internal appeal within 90 days of the agency's receipt of the appeal.

e. If a challenge is denied, the challenger will be made aware of their appeal rights to ISCAP.

5.4.2. Original Classification Authority (OCA). Agency personnel with OCA designation are identified in 14 CFR, Section 1203.800, Delegation of Authority to Make Determinations in Original Classification Matters. The following NASA personnel possess OCA designation:

5.4.2.1. NASA Administrator - Up to and including Top Secret.

5.4.2.2. Deputy Administrator - Up to and including Top Secret.

5.4.2.3. Associate Deputy Administrator - Up to and including Top Secret

5.4.2.4. Associate Deputy Administrator for Technical Programs - up to and including Top Secret.

5.4.2.5. Assistant Administrator for Security and Program Protection (AA/OSPP) - up to and including Top Secret.

5.4.2.6. Director, Security Management Division (DSMD) - up to and including Top Secret.

5.4.2.7. NASA Inspector General (Non-delegable) when so designated in writing - up to

Secret.

5.4.2.8. Center Chiefs of Security when so designated, in writing, by the AA/OSPP - up to Secret.

5.4.2.9. Other personnel, with sufficient justification, as designated in writing by the AA/OSPP - up to Secret.

5.4.3. Marking for Original Classification.

5.4.3.1. Personnel shall not designate information as classified (Confidential, Secret, or Top Secret) unless specifically approved by the CCS or an individual having OCA.

a. Physically marking classified information with the appropriate classification markings clearly warns and informs people of their responsibility to protect it.
b. Other notations facilitate downgrading, declassification, and aid in derivative classification actions.

5.4.3.2. Overall markings along with page, component, portion markings, and use of cover sheets shall conform to guidelines established by the CCS in accordance with EO 12958 and promulgated in Chapter 8, "Classified Correspondence," NPR 1450.10C, "NASA Correspondence Management and Communications Standards and Style."

5.4.3.3. Documents classified under any previous EO need not be remarked to comply with current marking requirements.

5.4.4. Marking for Derivative Classification.

5.4.4.1. Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the markings of the source information. The source information ordinarily consists of a classified document or documents, or a classification guide issued by an original classification authority. Persons who apply derivative classification markings shall observe and respect original classification decisions, carry forward to any newly created documents the pertinent classification and declassification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward, the date or event for declassification that corresponds to the longest period of classification among the sources and a listing of the sources on or attached to the official file or record copy. Users can also use classification guides for derivative classifying. Center Security Office will be prepared to provide assistance as requested. The CCS will ensure they have access to the ISOO Marking Classified National Security Information Pamphlet www.archives.gov/isoo/ and other guidance.

5.4.4.2. Markings other than "Top Secret", "Secret", and "Confidential," such as "For Official Use Only," "Sensitive But Unclassified," ":Limited Official Use," or "Sensitive Security Information," shall not be used to identify Classified National Security Information (CNSI). Foreign Government documents shall contain the country of origin or FGI. If the identity of the specific government must be concealed, the document shall be marked, "This Document Contains Foreign Government Information," and pertinent information marked "FGI", together with classification level, e.g., "(FGI-C)."

5.4.4.3. As required, the CCS shall develop and issue appropriate requirements on

derivative classification actions and procedures.

5.4.4.4. Mark documents containing Foreign Government Information with: "This document contains (country of origin) Information." Mark the portions that contain the foreign government information to indicate the country of origin and the classification level. Substitute the words "Foreign Government Information" or "FGI" in instance in which the identity of the specific government must be concealed. Note: If the fact that information is foreign government information must be concealed, the markings described here shall not be used and the document shall be marked as if it were wholly of U.S. origin. Your Center Security Office can provide you with information and pamphlets on how to properly mark all classified information.

5.4.5. Special Access Program (SAP) Markings. NASA employs SAP markings that are authorized and prescribed by the NASA Special Access Program Security Guide (SAPSG) concerning national security information for limiting access to cleared personnel having a need-to-know in the performance of their official duties.

5.4.6. Sensitive Compartmented Information (SCI). The NASA Special Security Office (SSO) must review for appropriate classification and marking any document for interagency use (MOU/MOA, Memorandum, or general correspondence) involving SCI or suspected SCI produced without the benefit of a specific classification guide.

5.4.7. Declassification and Downgrading.

5.4.7.1. In accordance with E.O. 12958, as amended, all Classified National Security Information (CNSI) records that (1) are more than 25 years old and (2) have been determined to have permanent historical value under Title 44, United States Code, shall be automatically declassified on December 31, 2006, whether or not the records have been reviewed. Subsequently, all classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of its original classification unless the information falls under one of the (9) exemption categories in E.O. 12958, as amended. If that is the case, a decision will be made to continue classification of the information. Pursuant to the Atomic Energy Act of 1954 as amended and 50 USC 435, all NASA Declassification Authorities (DCA) must successfully complete the Department of Energy (DoE) training on the recognition of restricted data and formerly restricted data (RD/FRD). Upon nomination to the AA/OSPP by an AA, or Center Director/Chief of Security, and completion of the required DoE training, individuals may be granted DCA.

5.4.7.2. The DSMD has developed the NASA Declassification Management Plan which provides the framework for NASA compliance with Section 3.3 through 3.7 of E.O. 12958, as amended. The NASA Declassification Plan will cover the following: Purpose, Legal Basis and Authority, 25 year Automatic Declassification, Systematic Declassification Review, Mandatory Declassification Review, Declassification Review Technique, RD/FRD review, Special Media Records, TS, TS/SCI, SAP Material review, Classification and Declassification Guides, Foreign Government Information, Declassification vs. Release, NASA Records Retention Schedule, NASA Handbook for Preparing Security Classification Guides, NASA Security Classification Guides, NASA Original Classification Authority, NASA Declassification Authority, Major Subject Matter/Equity Headings, Classification/Declassification Glossary, 25 year Automatic Declassification Exemptions, NASA Declassification Review and Referral Handbook, Review and Referral procedures, Declassification Authorities and NASA Staff contacts. NASA DCAs may only declassify NASA-originated classified national security information (CNSI).

5.4.7.3 An agency head may exempt from automatic declassification classified national security information, a group or file series "EXEMPT FILE SERIES" (A "file series" is also described in Information Security Oversight (ISOO) guidance as an "integral file block.") of records if the release of a substantial portion of the records within the file series would be expected to remain exempt based on the provisions of E.O. 12958, as amended, Section 3.3. (b) and (c). E.O. 12958, as amended, Section 3.3. (d) states: At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Panel, of any specific information beyond that included in a notification to the President under paragraph (c) E.O. 12958, as amended, Section 3.3., that the agency proposes to exempt from automatic declassification. File series exemptions were approved by ISOO in 1996 pursuant to the E.O.12958, signed in April 1995, and did not have to be re-approved under E.O. 12958, as amended, signed in March 2003. File series exemption criteria include the following:

a. a description of the information, either by reference to information in specific records or in the form of a declassification guide

b. an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time

c. except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b) of E.O. 12958, as amended, Section 3.3., a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

5.4.7.4. The following Agency personnel have declassification and downgrading authority.

5.4.7.4.1. As OCAs for the Agency, individuals listed in 5.4.2.1. through 5.4.2.6. are also authorized to declassify NASA-originated CNSI.

5.4.7.4.2. Other individuals who hold a signed letter of designation as a DCA for their directorate, office, or Center. All letters of designation must be signed by the AA/OSPP.

5.4.8. When conducting yearly reviews of classified holdings for automatic declassification as required under EO 12958, the CCS shall ensure declassification authority is assigned, per subparagraph 1.1.7.11, to qualified federal employee personnel subject matter experts and shall assist them in declassification efforts, as appropriate.

5.5 Access to CNSI

5.5.1. At a minimum, NASA personnel and other individuals associated by contract or other agreement shall meet the following criteria for accessing CNSI:

5.5.1.1. Possess a personnel security clearance commensurate with the required access. (Reference chapter 2 and chapter 6 of this NPR).

5.5.1.2. Have a justified need-to-know.

5.5.1.3. Must have signed an official nondisclosure statement (SF 312) witnessed by a NASA security official.

5.6 Accountability and Control of CNSI

5.6.1. Accountability of classified information is essential to maintaining a history of what you have, where it is, and who has it. Through effective accounting procedures it must be possible to trace the movement and detect the loss of classified information in a timely manner.

5.6.1.1. All CNSI information shall be strictly accounted for and covered by a continuous chain of signature receipts. However, this chapter represents the MINIMUM requirements for accountability and control. Centers are encouraged to implement additional controls they deem appropriate.

5.6.1.2. Each Center shall have an information management system and set of written procedures to control the classified information in its possession. The system or procedures shall contain specific requirements for accounting and safeguarding CNSI. The system shall be sufficient to reasonably preclude the possibility of its loss or compromise.

5.6.2. A trained Top Secret Control Officer (TSCO) and Alternate shall be designated, in writing, by the Center Director or CCS. The TSCO shall ensure that all Center TS material is accounted for, protected, and transmitted under a chain of receipts using NASA Form 387, "Classified Material Receipt," identifying each individual with custody of the material.

5.6.3. A trained Classified Material Control Officer (CMCO) and Alternate shall be designated in writing by the Center Director or CCS. The CMCO shall ensure that all Center CNSI material is accounted for, protected, and transmitted under a chain of receipts using NASA Form 387, "Classified Material Receipt," for each individual with custody of the material. Upon written designation by the Center Director or CCS, the CMCO, as well as his/her alternate, may also serve as the TSCO.

5.6.3.1. The CMCO is responsible to the CCS for the Center Security Control Point (SCP) and oversight of the Document Control Stations (DCS) within the Center and/or facilities.

5.6.3.2. Establishment of Security Control Point (SCP). One SCP, operated by the CMCO, shall be established within each Center or facility that has a requirement to handle classified information. The SCP shall be designated in writing within the local security Procedural Requirements. All incoming and outgoing classified information shall be processed through the SCP with the following exceptions: Sensitive Compartmented Information (SCI) material, CMS material, and classified messages that are handled, processed, and stored within secure telecommunications spaces.

5.6.3.3. Document Control Station (DCS). At a Center with a significant volume of classified material and where the SCP serves many organizations, each organization which has or shall have custody of classified material shall establish a DCS run by a Document Control Station Officer (DCSO). Organizationally, this station may be established at the office, division, staff or lower level depending upon the circumstances. Creation of such stations shall be coordinated with the CMCO, and approved in writing by the CCS.

5.6.4. Accountability records.

5.6.4.1. All CNSI must be accounted for throughout its lifecycle. Records shall be maintained for all CNSI and retained for five years after final disposition. These records shall be maintained at the SCP for any accountable information which is received, generated, reproduced, transmitted, downgraded, or destroyed. A Classified Document Control Log shall be used for this purpose.

5.6.4.2. The Document Control Log maintained at the SCP shall at a minimum reflect the following:

a. Date of receipt and date of origination.
b. Agency/installation from which received or by which originated.
c. Classification level of the material.
d. A brief unclassified title or description of the material.
e. The date of declassification or downgrading.
f. Control number assigned. Each copy of a classified document or item shall have its own control number. Copy numbers shall not be used as part of the control number.
g. Information indicating the location or local holder of the material. (Local holders/custodians shall have some form of signature receipt on file acknowledging that they have custody of the material).
h. Disposition and date for all material destroyed, downgraded, declassified, or dispatched outside the installation.

5.6.4.3. The Document Control Log maintained at the DCS shall at a minimum reflect the following:

1. (1) Classification level of the material.
2. (2) Control number assigned.
3. (3) Disposition and date for all material destroyed, downgraded, declassified or dispatched outside of the DCS.

5.6.4.4. Accountability records shall also contain signed receipts and destruction reports. Signed receipts and destruction reports shall be retained for four years after final disposition.

5.6.5. Top Secret disclosure records.

5.6.5.1. A disclosure record of all persons who are afforded access (visual, oral, record copies, etc.) to Top Secret information (except safe combinations) shall be maintained. This record shall show the names of all individuals given access and the date of such access. To comply with this requirement, a Top Secret Cover Sheet (Form SF 703) shall be attached to all Top Secret information in document form. For access given orally, a log listing the required information shall be maintained. At a minimum, the Disclosure Record Sheet shall provide:

a. Information reflecting the document being disclosed;

b. Individual to whom the information is being disclosed;

c. Organization and Telephone Number; and

d. Date the information is disclosed.

5.6.5.2. Records shall be retained for five years from the date of final disposition.

5.6.6. Exceptions from accountability.

5.6.6.1. Electronic Processing: Installations that electronically process Confidential and Secret information, including e-mail, within a designated restricted area that meets the security requirements of a classified space in accordance with this manual are authorized an exception from the requirement to account for that information under the following conditions:

a. They shall account for IT storage media.

b. They shall account for all Confidential and Secret material that is transferred or distributed outside the classified space.

c. When a classified IT system is used, print only that material that is operationally required to be "hard copy." Conspicuously mark the "hard copy" to indicate the installation and office printing the copy.

d. They shall limit the number of personnel authorized to print classified material from a classified IT system.

e. They shall ensure that all Confidential and Secret material is destroyed by an approved method.

f. They ensure quarterly refresher security briefs are conducted and documented for all personnel working in the classified space. The intent is to increase security awareness to compensate for these relaxed security requirements.

g. They shall establish written procedures approved by the CCS to ensure compliance with the above requirements. These procedures may be included in the unit's information security plan discussed in this manual.

5.6.6.2. This exception does not apply to any other accountable Confidential and Secret material stored within the classified space.

5.6.7. Receipt of classified material.

5.6.7.1. The CCS shall provide written procedures for the handling of incoming classified material. When a Center/facility receives incoming mail, bulk shipments, and items delivered by messenger, the following controls shall be implemented:

1. All classified material shall be delivered promptly to the SCP or properly safeguarded in accordance with this manual until delivery to the SCP can be effected.

2. All Registered, USPS Express mail, and contract (FEDEX, etc.) overnight delivery packages shall be delivered unopened to the SCP and protected as Secret material until determined otherwise.

3. All personnel who open official mail of any sort shall be directed to immediately

deliver any classified material to the SCP. Outer wrappers along with the UNOPENED inner wrapper shall be delivered to the SCP. If an individual opens mail which is not correctly packaged, causing exposure to uncleared or unauthorized individuals, the material shall be delivered to the SCP, and the CCS shall be notified. The CCS shall investigate and submit a report of incidents involving classified material outlined in paragraph 5.19 of this chapter.

4. All incoming packages containing classified material shall be inspected for tampering. If tampering is discovered, it shall be reported to the CCS who shall conduct such inquires as are necessary. The contents of the package shall be checked against the enclosed receipt.

5. Incoming classified information that does not fall under the CMC system shall be processed in accordance with the procedures established for that type of material (e.g., COMSEC, NATO).

5.6.8. Record of destruction.

5.6.8.1. An accurate record of destruction of classified material is as important as its destruction. Proper accounting procedures, together with accurate records of destruction, provide evidence of the proper disposition of classified material. Records of destruction shall be retained for 4 years.

5.6.8.2. A record of destruction is required for all CNSI material. The destruction record shall indicate the date the material was actually destroyed, the control number, the short title or a description of the material destroyed consistent with the description indicated in the control log, and the printed names and signatures of the official actually performing the destruction and a witness. Both individuals must have personal knowledge of the actual material destroyed. If applicable, the official authorizing the destruction shall also sign the record. Either the control log or a separate destruction report may be used for this purpose.

5.6.9. Inventory requirements.

5.6.9.1. Two appropriately cleared individuals shall conduct inventories. One of the individuals may be the control officer for the material. However, the other individual must be an appropriately cleared, disinterested party not involved in the operation of the account.

5.6.9.2. An inventory is a visual sighting of each item of accountable material. All documents held shall be checked to ensure that they are entered into accountability, and all documents entered into accountability shall be sighted, including those items signed out on local custody. If no disposition can be determined, an incident involving classified material shall be submitted in accordance with paragraph of this chapter.

5.6.9.3. All Top Secret holdings shall be inventoried upon change of custodian or semiannually. Semiannual inventories may be combined with change of custodian inventories. Accountability records shall also be reviewed for accuracy and continuity. See section 5.7 for a complete listing of required page checks.

5.6.9.4. All Secret and Confidential holdings shall be inventoried upon change of custodian or annually. Annual inventories may be combined with change of custodian inventories. In those instances where exceptionally large holdings (more than 500 control numbers) make conducting an annual inventory difficult, Centers may complete

the inventory of material over a 3-month period. An inventory is not required for material authorized for an exception to the accountability requirements listed in section 5.6.4. Top Secret material must be inventoried semi-annually. One inventory may be conducted in conjunction with the scheduled annual inventory of Secret and Confidential material.

5.6.9.5. The Center shall retain a record of all inventories for a period of at least five years. An inventory and a report of the results, including any discrepancies discovered, shall be forwarded annually to the cognizant CCS. Although an inventory of Top Secret holdings is required on a semi-annual basis, a written report to the CCS is only required annually unless discrepancies are discovered. Although the Top Secret inventory is only reported annually, local documentation of all inventories must be maintained at the installation as described above.

5.6.9.6. Upon change of custodian, all classified material shall be transferred to the new custodian. A joint inventory shall be conducted, accounting for each item. Both parties shall sign the report.

5.6.10. Changes and corrections

The custodian, under the direction of the CMCO, shall be responsible for the entry of all changes and corrections to the material in their custody. A Publication Change Checklist must be used for all changes entered. Completed checklists shall be retained until the publication is destroyed or superseded.

5.7 Page Checks

5.7.1. A page check shall be conducted on all Top Secret (TS) material. Page checks involve visually sighting each page in a document, verifying its presence against a list of effective pages (if applicable), and ensuring that the page is from the correct change. In the absence of a list of effective pages, the document shall be examined for continuity. After each page check, the individual shall sign the page check record (except for page checks prior to destruction). If one does not exist, a page check record shall be produced locally and kept with the publication. The record shall identify the publication, the name of the individual conducting the page check, discrepancies noted, and the date of the check.

5.7.2. Page checks on TS material shall be conducted on the following occasions:

Initial receipt	Yes
Page change	Yes
Change residue	Yes
Change of custodian	Yes
Inventory	Yes
Destruction	Yes

5.7.3. Page checks on Secret material shall be conducted on the following occasions:

Initial receipt	Yes

Page change	Yes
Change residue	Yes
Change of custodian	Yes
Inventory	No
Destruction	Yes

5.7.4. No page checks are required for Confidential material.

5.8 Working Papers

5.8.1. Working papers are documents, including drafts, notes, photographs, computer media, etc., accumulated, created, or received electronically to assist in the formulation and preparation of a finished document. Classifying as "working papers" is not intended as a way around the original classification procedure or temporary classification. Working papers, which contain classified information produced by a unit shall be:

5.8.1.1. Dated when created.

5.8.1.2. Marked with the highest classification of information contained in the document.

5.8.1.3. Protected in accordance with the classification assigned.

5.8.1.4. After 180 days, material classified as working papers must be destroyed or correctly classified by an original classification authority.

5.8.2. The accounting, control, and marking requirements prescribed for a finished document shall be followed when working papers contain Top Secret information or are:

5.8.2.1. Released by the originator outside the NASA facility or transmitted electronically.

5.8.2.2. Retained more than 90 days from the date of origin, and

5.8.2.3. Filed permanently.

5.9 Storage of CNSI, NATO and Classified Foreign Government Material.

5.9.1. All classified documents and material under the jurisdiction of NASA shall be stored in a "General Services Administration Approved" Security Container with an approved combination lock or approved facility/room with sufficient physical and procedural security measures to preclude unauthorized access. Whenever new security equipment is procured, it shall be in conformance with the standards and specifications established by the Administrator of General Services, and shall, to the maximum extent possible, be of the type available through the Federal Supply System. See section 5.21 for requirements on security container management. The CCS shall ensure that adequate storage is available for CNSI in accordance with applicable NASA and federal regulations.

5.9.2. Each Center shall apply the following:

5.9.2.1. Mandatory use of Standard Form (SF) 702-101, "Security Container Sheet."

5.9.2.2. Combinations shall be changed when first placed in service and then as needed whenever a person knowing the combination is transferred or terminated from employment or for some other reason is no longer authorized access to the classified material stored in the equipment or area; whenever it is possible that the combination may have been subjected to compromise; or whenever the security storage equipment or security area has been found unsecured and unattended.

5.9.2.3. NATO classified information shall be safeguarded in compliance with United States Security Authority for NATO Instructions I-69 and I-70. Foreign Government information should be stored separately from other classified information. To avoid additional costs, separate storage may be accomplished by methods such as separate drawers of a container. Safeguarding standards may be modified if required or permitted by treaties or agreements, or for other obligations, with prior written consent of the National Security Authority of the originating government, hereafter "originating government. Please see ISOO Directive No.1 for more detail on how to protect foreign government information.

5.9.2.4. Agency heads or any designee may prescribe special provisions for the dissemination, transmission, safeguarding and destruction of classified information during certain emergency situations. In emergency situations, in which there is an imminent threat to life or in defense of the homeland, agency heads or designees may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access under the following conditions:

a. Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose

b. Limit the number of individuals who receive it

c.Transmit the classified information via approved Federal Government channels by the most secure and expeditious method to include those required in subpart C of ISOO Directive No.1, or other means deemed necessary when time is of the essence.

d. Provide instructions about what specific information is classified, how it should be safeguarded; physical custody of classified information must remain with an authorized Federal Government entity, in all but the most extraordinary circumstances

e. Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed nondisclosure agreement

f. Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 30 days after the release, the disclosing authority must notify the originating agency of the information by providing the following information:

1. A description of the disclosed information

2. Who authorized the disclosure

3. .To whom the information was disclosed

4. How the information was disclosed and transmitted

5. Reason for the emergency release

6. How the information is being safeguarded

7. A description of the briefing provided and a copy of the nondisclosure agreements signed.

5.10 Reproduction of CNSI

5.10.1. Reproduction of classified information and material must be kept to a minimum. Only equipment designated by the CCS is authorized to reproduce classified information. Each Center CCS shall develop and implement written procedures to ensure that the following requirements, as a minimum, are met:

5.10.1.1. Protect classified information during reproduction.

5.10.1.2. Adequately clear equipment after reproduction.

5.10.1.3. Ensure reproduced copies are incorporated into the Center CNSI accountability system.

5.10.1.4. Safeguard overruns, waste, and blank copies generated during the clearing of reproduction equipment as classified material and destroy accordingly.

5.10.1.5. Ensure security procedures are provided for reproducing classified information by other technical means.

5.11 Hand Carrying and Receipting of Classified Material

5.11.1. CNSI shall be transmitted in a manner that ensures protection of the material. A receipt shall be required whenever CNSI material is transmitted using an internal mail routing system, entered in the U.S. Postal System or via authorized contract courier, transmitted off the Center by any means, transmitted to a non-NASA activity, or when the transmitting custodian wishes to verify change of custody.

5.11.2. Methods of Transportation within a Center.

5.11.2.1. The TSCO, custodian, or other employee having a Top Secret clearance and designated by either TSCO or the CCS, shall personally hand-carry Top Secret information within a Center. A Top Secret Cover Sheet (Form SF 703) shall be attached to all Top Secret information in document form.

5.11.2.2. When traveling within a building or between buildings on a Center, classified material shall be hand carried covered with the appropriate coversheet and enclosed in a single envelope or other suitable package marked with the highest classification or carried in a briefcase or other container. When hand carrying classified material, the individual shall proceed directly to the intended destination. Restroom breaks, coffee breaks, etc., are not permitted when hand carrying classified material.

5.11.2.3. Between buildings of a Center that are widely dispersed or between buildings occupied by NASA and located in metropolitan areas, Top Secret information shall be transmitted within double-wrapped, appropriately marked, and addressed envelopes as prescribed in paragraph 5.11.3 below or in a manner approved by the CCS.

5.11.2.4. Additional measures may be established by the CCS to control access to any CNSI by an unauthorized person during transmission.

5.11.2.5. Such material shall be transmitted inside a Center by hand-delivery from an employee possessing a clearance at least as high as the category of classification of the material involved.

5.11.3. Hand Carrying Outside a Center.

5.11.3.1. The DSMD or the CCS shall appoint a NASA employee or contractor to be a designated courier of CNSI when it is essential for that NASA employee or contractor to hand carry such information outside HQ or a Center.

5.11.3.2. Couriers may also be required for symposiums where transport, control, and access to CNSI may be necessary, for "cleared" conference or symposium attendees, including other agency personnel, or NASA contractors holding NASA security clearances under a NASA DD Form 254.

5.11.3.3. Designated couriers shall be briefed that classified material must be in their physical possession at all times (i.e., not in checked baggage, left unattended in hotel room or vehicles, safeguarded in hotel safety boxes, or taken to bars, dining, or places of entertainment) and protected from opening, examination, or inspection. Furthermore, designated couriers must acknowledge that their authorization to courier CNSI is only valid within the United States of America and its territories.

5.11.3.4. Authorization shall be provided to the designated courier on letterhead NASA stationery, marked "Valid only in the United States of America," and shall include a specific expiration date and the names and home telephone numbers of two NASA Security Specialists who may be contacted if the designated courier is challenged to open the materials by non-NASA personnel (e.g., police, other Government officials, or airline personnel).

5.11.3.5. Personnel shall be briefed on Advisory Circular, "Federal Aviation Administration, Subject: Screening of Persons carrying U.S. Classified Material, AC 108-3."

5.11.3.6. CNSI transmitted outside a Center shall be enclosed in an envelope with opaque inner and outer covers. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents.

5.11.3.7. A receipt shall be attached to or enclosed in the inner cover. It shall identify the sender, the addressee, and a description of the materials being transmitted. It shall be signed by the recipient, returned to the sender, and retained for two years.

5.11.3.8. A suspense system shall be established to track transmitted documents until a signed copy of the receipt is returned. If signed receipts are not received within 30 days of transmission of the material, the DCSO or CMCO shall report the non-receipt to the CCS.

5.11.3.9. When the material is of a size, weight, or nature that precludes the use of envelopes, the materials used for packaging shall be of such strength and durability to ensure the necessary protection while the material is in transit.

5.12 Transmission of Classified Material

5.12.1. The term "transmission" refers to any movement of classified material or material from one place to another. Unless a specific kind of transportation is restricted, the means of transportation is not significant.

5.12.1.1. Classified material shall be transmitted either in the custody of an appropriately cleared individual, by an approved system or courier, or otherwise in accordance with the provisions of this chapter.

5.12.1.2. The carrying of classified material across national borders is not permitted unless arrangements have been made that shall preclude customs, postal, or other inspections. In addition, foreign carriers may not be used unless the U. S. escort has physical control of the classified material.

5.12.2. Top Secret transmission. Neither the normal mail or messenger system of an Installation nor postal and commercial delivery services are authorized for the transmission of Top Secret material. Top Secret material shall only be transmitted by:

5.12.2.1. Defense Courier Service (DCS).

5.12.2.2. Department of State Courier System.

5.12.2.3. Appropriately cleared NASA civilian personnel specifically designated as a courier.

5.12.2.4. Telecommunications systems specifically approved for transmission of Top Secret material.

5.12.3. Secret transmission. Transmission of Secret material may be effected by:

5.12.3.1. Any of the means approved for the transmission of Top Secret, except that Secret material, other than that containing cryptological information, may be introduced into the DCS only when the control of such material cannot otherwise be maintained in U. S. custody. This restriction on use of the DCS does not apply to Sensitive Compartmented Information (SCI) and Communications Security (COMSEC) material. When the Department of State Courier System is to be used for transmission of Secret material, the Secret material shall be sent by registered mail to the State Department Pouch Room.

5.12.3.3. U. S. Postal Service (USPS) registered mail within and between the 50 United States and its Territories.

5.12.3.4. USPS Express Mail Service may be used between NASA units and contractors within and between the 50 United States and its Territories. USPS Express Mail is authorized only when it is the most cost effective method or when time/mission constraints require it. The package shall be properly prepared for mailing. The USPS Express Mail envelope shall not serve as the outer wrapper. Under no circumstances shall the sender execute the "WAIVER OF SIGNATURE AND INDEMNITY" section of the USPS Express Mail Label for classified material. This action can result in drop-off of a package without the receiver's signature and possible loss of control.

5.12.3.5. When an urgent requirement exists for overnight delivery within the 50 United States and its Territories, the Center Director may authorize the CCS to use Federal Express (FedEX) for overnight delivery of material for the Executive Branch. The sender is responsible for ensuring that an authorized person shall be available to receive the delivery. The package may only be addressed to the recipient by name. The release

signature block on the receipt label shall not be executed under any circumstances. The use of street-side collection boxes is prohibited. COMSEC, NATO, and foreign government information (FGI) shall not be transmitted in this manner.

5.12.3.6. Outside the area described in subparagraph 5.12.3.5 above, Secret material may be moved by USPS registered mail through Army, Navy or Air Force Postal Service facilities provided that the material does not pass through a foreign postal system or any foreign inspection, or via foreign airlines. The material must remain under U. S. control. Special care shall be taken when sending classified material to U. S. activities overseas. If the material is introduced into a foreign postal system, it has been subjected to compromise.

5.12.3.7. Within U. S. boundaries only, qualified carriers authorized to transport Secret material via a Protective Security Service (PSS) under the National Industrial Security Program. This method is authorized only when the size, bulk, weight, nature of the shipment or escort considerations make the use of other means impractical.

5.12.3.8. Other carriers under escort of appropriately cleared personnel. Carriers included are Government and Government contract vehicles, aircraft, ships of the U.S. Navy, Federal employee-manned U.S. Naval Ships, and ships of U. S. registry. Appropriately cleared operators of vehicles, officers of ships, or pilots of aircraft who are U. S. citizens may be designated as escorts provided the control and surveillance of the carrier is maintained on a 24-hour basis. The escort shall protect the shipment at all times, through personal observation or authorized storage to prevent inspection, tampering, pilferage or unauthorized access until delivery to the consignee. However, observation of the shipment is not required during the period if stored in an aircraft or shipped in connection with , flight or se , a transit, provided the shipment is loaded into a compartment that is not accessible to any unauthorized persons aboard or loaded in specialized shipping containers, including closed cargo containers.

5.12.3.9. Telecommunications systems specifically approved for the transmission of Secret material.

5.12.4. Confidential transmission. Transmission of Confidential material may be effected by:

5.12.4.1. Any of the means approved for the transmission of Secret material.

5.12.4.2. USPS registered mail for:

a. Confidential COMSEC, NATO, and other special category material.

b. Other Confidential material to and from Fleet Post Office (FPO) or Army Post Office (APO) addressees located outside the U. S. and its Territories.

c. Other addressees when the originator is uncertain that their location is within the U. S. boundaries. Use of return postal receipts is not authorized. If considered desirable, a document receipt may be used.

d. When the sender deems it necessary to ensure adequate protection of the classified material.

5.12.4.3. USPS First Class mail between NASA and other U.S. Government agency locations anywhere in the U. S. and its territories. However, the outer envelope/wrappers of such Confidential material shall be marked "FIRST CLASS," and

endorsed "RETURN SERVICE REQUESTED."

5.12.4.4. Certified or, if appropriate, registered mail shall be used for material directed to contractors and to agencies of the Executive Branch.

5.12.4.5. Within U. S. boundaries, commercial carriers that provide a Signature Security Service (SSS). This method is authorized only when the size, bulk, weight, nature of shipment, or escort considerations make the use of other methods impractical.

5.12.4.6. In the custody of commanders or masters of ships of U. S. registry who are U. S. citizens. Confidential material shipped on ships of U. S. registry may not pass from U.S. Government control. The commanders or masters must give and receive classified material receipts and agree to:

a. Deny access to the Confidential material by unauthorized persons, including customs inspectors, with the understanding that Confidential cargo that would be subject to customs inspection shall not be unloaded; and

b. Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.

5.13 Release of Classified Information to Foreign Governments

5.13.1. Subsequent to a determination by the DSMD that classified material may be released to a foreign government; the material shall be transferred between authorized representatives of each government in compliance with the provisions of this chapter. To assure compliance, each contract, agreement, or other arrangement that involves the release of classified material to foreign entities shall either contain transmission instructions or require that a separate transportation plan be approved by the DSMD prior to release of the material. Classified material shall be transmitted only:

a. To an embassy or other official agency of the recipient government which has extraterritorial status; or

b. For on-loading aboard a ship, aircraft, or other carrier designated by the recipient government at the point of departure from the U. S. or its territories or possessions, provided that at the time of delivery a duly authorized representative of the recipient government is present at the point of departure to accept delivery, ensure immediate loading, and to assume security responsibility for the classified material.

5.13.2. Classified material to be released directly to a foreign government representative shall be delivered or transmitted only to a person who has been designated in writing by the recipient government as its officer, agent, or employee. This written designation shall contain assurances that such person has a security clearance at the appropriate level and that the person shall assume full security responsibility for the material on behalf of the foreign government. The recipient shall be required to execute a receipt for the material, regardless of the level of classification.

5.13.3. Each contract, agreement, or arrangement, which contemplates transfer of U. S. classified material to a foreign government within the U. S. or its territories, shall designate a point of delivery in accordance with subparagraph 5.13.1.a. or 5.13.1.b. If

delivery is to be made at a point described in subparagraph 5.13.1.a., the contract, agreement, or arrangement shall provide for U. S. Government storage or storage by a cleared contractor at or near the delivery point so that the U. S. classified material may be temporarily stored in the event the carrier designated by the recipient foreign government is not available for loading. Any storage facility used or designated for this purpose must afford the U. S. classified material the protection required by this manual.

5.13.4. If U. S. classified material is to be delivered to a foreign government within the recipient country, it shall be transmitted in accordance with this chapter. Unless a designated or approved courier or escort accompanies the material, it shall, upon arrival in the recipient country, be delivered to a U. S. Government representative who shall arrange for transfer to a duly authorized representative of the recipient foreign government.

5.14 Receipt System

5.14.1. Top Secret material shall be transmitted under a continuous chain of signed receipts.

5.14.2. Secret and Confidential material shall be covered by a receipt between installations and other authorized addressees and between custodians within the same Center/facility.

5.14.3. Receipts shall be provided by the transferring installation, and the forms shall be attached or enclosed in the inner envelope or cover. Domestic Return Receipt form, PS Form 3811, or NASA Form 287 (Classified Material Receipt) or a facsimile shall be used for this purpose.

5.14.4. Receipt forms shall be unclassified and contain only such information as is necessary to identify the material being transmitted.

5.14.5. A duplicate copy of the receipt shall be retained in a suspense file until the signed original is returned. If a signed receipt is not received within 45 days, follow-up action shall be initiated and the cognizant CCS shall be informed.

5.14.6. Copies of signed receipts shall be retained for a period of 4 years.

5.15 Managing and Handling COMSEC Material

Pending issuance of separate specific NASA COMSEC Policy and Procedures, users of COMSEC material shall follow the requirements in managing and handling COMSEC material established in the NASA Central Office of Record Standard Operating Procedures (CSOP) and the National Security Telecommunications Systems Security Instruction (NSTSSI) 4005. The Center COMSEC Officer shall serve as the focal point for all COMSEC issues.

5.16 Defense Courier Service Reimbursement Program

Upon request of the AA/OSPP, the CCS shall provide information on the Center's use of the reimbursable service of the Defense Courier Service (DCS) for transmitting CNSI outside the Center.

5.17 Disposition or Destruction of Classified Material

5.17.1 Inactive CNSI shall be disposed of in accordance with NPR 1441.1, NASA Records Retention Schedules. Each Center shall employ security procedures and methods for destruction, witnessing, certification, and retention of CNSI in accordance with this chapter.

5.17.2 Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information.

5.17.3. Installations shall continuously review their classified holdings. Classified information shall be destroyed when determined to be no longer required for operational or administrative purposes. The Center CCS shall establish annual Centerwide classified material destruction events to ensure classified holdings are properly reviewed and unneeded CNSI disposed of in accordance with NPR 1441.1, NASA Records Retention Schedules. Custodians of classified material deemed no longer viable shall be required to destroy it or transfer to a Center technical library. Collecting or hoarding CNSI is prohibited.

5.17.4. Additional policy must be followed when destroying Communications Security (COMSEC) material as contained in approved CSOPs and NSTSSI 4005.

5.17.5. NASA ACI or For Official Use Only (FOUO) that cannot be decontrolled or that which is no longer needed shall be deleted from IT systems and shredded, burned, or destroyed in other similar methods that preclude unauthorized disclosure.

5.17.6. Unclassified material, including formerly classified material that has been declassified, unclassified messages, and ACI material, does not require the same assurances of complete destruction. To avoid overloading an installation's classified material destruction system, unclassified material shall be introduced only when the CCS or higher authority determines it to be required because of unusual security considerations or efficiency.

5.17.7. Approved destruction methods. Destruction devices must be approved by NSA, as listed in NTISSI 4004 Annex B, NSA Evaluated Destruction Devices. Pulpers, pulverizers, or shredders may be used for the destruction of paper products and some forms of computer media. Only paper-based products may be destroyed by pulping. Classified material in microform, that is, microfilm, microfiche, or similar high data density material, may be destroyed by burning or chemical decomposition or other methods as approved by the cognizant CCS. Equipment approved for the destruction of classified material shall be operated properly and provided with regular maintenance, as suggested by the manufacturer. The following are the approved methods for the destruction of classified material:

5.17.7.1. Burning. When burning is used for destruction of classified information, steps shall be taken to ensure that the wind or draft does not carry portions of burned material away and that the resulting ash is broken up sufficiently to preclude reconstruction.

5.17.7.2. Shredding. Any crosscut shredder whose residue particle size is equal to or smaller than 1/32 of an inch in width by 1/2 inch in length (1/32 x 1/2 is approved for the destruction of all classified paper material, magnetic tape, and cards. Shredders shall not be used to destroy classified microfilm, microfiche or similar high information density human readable material. THIS DOES NOT INCLUDE COMSEC ITEMS WHICH MUST BE DESTROYED IN ACCORDANCE WITH ESTABLISHED NATIONAL SECURITY AGENCY (NSA) REQUIREMENTS CONTAINED IN COMMITTEE ON NATIONAL

SECURITY SYSTEMS (CNSS) POLICY NO. 16, DATED OCTOBER 2002. (NOTE: THESE NSA REQUIREMENTS WILL BE MAINTAINED AT CENTER SECURITY OFFICES.)

5.17.7.3. Pulping (Wet Process). Wet process pulpers with a 1/4 inch or smaller security screen may be used to destroy classified water-soluble material. Since pulpers only destroy paper products, staples, paper clips, and other fasteners shall be removed to prevent clogging the security screens.

5.17.7.4. Pulverizing (Dry Process). Pulverizers and disintegrators designed for destroying classified material are usually too noisy and dusty for office use, unless installed in a noise- and dust-proof enclosure. Some pulverizers and disintegrators may be used to destroy photographs, film, typewriter ribbons, magnetic tape, flexible diskette (floppy disk), glass slides, and offset printing plates. Pulverizers and disintegrators shall have a 3/32-inch or smaller security screen.

5.17.7.5. Chemical. Classified microfilm or microfiche may be destroyed by chemical process (e.g., put in an acetone bath).

5.17.7.6. Destruction of Classified Equipment. All components of classified equipment shall be destroyed by any method that destroys them beyond recognition.

5.17.7.7. Eradication of Magnetic Media. Destruction of classified Automated Information System (AIS) magnetic media shall be in accordance with established NASA requirements. A record of destruction records must be executed upon eradication of the classified information.

5.18 Destruction Procedures

5.18.1. Classified material shall only be destroyed by authorized means by individuals cleared to the level of the material being destroyed. A minimum of two individuals shall be responsible for destroying CNSI material, one of whom is a witness to the destruction. These individuals must have personal knowledge of the actual material destroyed (e.g., must positively identify the data which is to be destroyed).

5.18.2. The personnel tasked with the destruction or preparation for destruction of classified material shall be thoroughly familiar with the requirements and procedures for safeguarding classified information. They shall be thoroughly briefed on the following:

5.18.2.1. Safeguarding all classified material entrusted to them for destruction.

5.18.2.2. Conducting a thorough page check before destruction is accomplished.

5.18.2.3. Observing all documents destroyed or being prepared for destruction and checking the residue of locally destroyed material to ensure that destruction is complete and reconstruction is impossible.

5.18.2.4. Taking precautions to prevent classified material or burning portions of classified material from being carried away by wind or draft.

5.18.2.5. Completing and signing all appropriate records of destruction.

5.18.3. Classified waste. Classified waste shall be destroyed as soon as practicable. Containers used for the accumulation of Secret classified waste shall be dated when the first item of classified waste is deposited. If, after 30 days, the classified waste has not

been destroyed, it shall be entered into the accountability records of the SCP. It is not necessary to identify the individual items of classified waste when entering the waste into accountability. It is sufficient to identify simply as one container, for example, "box and bag etc., Secret classified waste." When destruction is completed, a record of destruction shall be prepared.

5.18.4. The CCS and AA/OSPP shall review or direct a review, at least annually, of Center classified material holdings expressly for the purpose of reducing to an absolute minimum the quantity on hand. A specific period shall be designated each year for classified material review and destruction. Custodians of CNSI shall be encouraged to dispose of classified holdings that are no longer relevant to ongoing research. Holding non-essential and outdated material poses storage and accountability problems that lead to loss and/or compromises as the owner soon loses track of the material. The CCS shall provide information on annual CNSI reduction efforts in accordance with paragraph 5.3 this chapter.

5.19 Security Violations and Compromise of CNSI

5.19.1. The CCS shall ensure that written procedures exist for the following:

5.19.1.1. Emergency action and reporting requirements for the loss of CNSI.

5.19.1.2. Action to be taken by the CCS in the event of the loss of control over CNSI.

5.19.1.3. Action required in the event that the lost CNSI was not compromised.

5.19.1.4. Action required in the event of possible compromise of CNSI.

5.19.1.5. Action required in the event of unauthorized disclosure of CNSI by NASA or contractor personnel.

5.19.1.6. Notification to the DSMD and the CAF when classified information is presumed compromised.

5.19.2. A written incident report shall be made to the DSMD on all issues as described in 5.19.1.

5.19.2.1. An initial report of incident involving classified material requires an immediate notification and presentation of the facts for the purpose of limiting and assessing the damage to the national security. The initial report shall be made to the DSMD within two working days. The intent is to notify all cognizant officials as soon as possible to limit further damage, assess weaknesses and correct a discrepancy, if appropriate. If a formal report cannot be accomplished in two days, the DSMD shall be provided with electronic mail that briefly describes the incident, immediate actions taken, and those planned.

5.19.2.2. Reports of incidents involving classified information shall contain the following information:

1. Type of report:

a. Compromise; or

b. Possible Compromise; or

c. Administrative Discrepancy.

2. Type of incident:

a. Compromise or Possible compromise;

1. Improper Destruction; or
2. Unauthorized access; or
3. Improper transmission (transmission via non-secure means or use of unauthorized equipment); or
4. Improper storage; or
5. Loss of material; or
6. Found material (material not in accountability system or previously
7. reported as lost) not subjected to possible compromise; or
8. Other (explain).

b. Administrative Discrepancy;

1. Mailed via non-registered/certified mail; or
2. Sent in single container; or
3. Markings on outer container divulged classification of contents; or
4. Classification not marked on inner container; or
5. No return receipt; or
6. Inadequate wrapping: not securely wrapped or protected; or
7. Received in poor condition: compromise improbable; or
8. Addressed improperly; or
9. Classified by unauthorized original classifier; or
10. Markings incorrect; or
11. Classified by, reason for classification, or declassify on, incorrect or missing (originally classified documents); or
12. Derived from or declassify on line incorrect or missing (derivatively classified documents); or
13. Other (explain).

3. Complete identification of all material involved including;

a. Unclassified title
b. Classification
c. Originator

4. Identity of all personnel involved including;

a. Full name
b. SSN
c. Security Clearance
d. Basis of Security Clearance

5. A statement of actions taken upon discovery of incident and description of events.
6. Weakness leading to the incident.
7. Corrective actions taken and actions taken to preclude recurrence.
8. Disciplinary action taken, if any.
9. Unit incident number, to include.

a. Fiscal year
b. Sequential number

5.19.2.3. The CCS shall submit a final incident report within 30 days of the incident. The report shall include:

a. Likelihood CNSI was compromised (provide details supporting determination).
b. Make general comments (may include authority to remove material from accountability or request further information).
c. Incident closure or further investigation required.
d. Center incident number (to include fiscal year and sequential number).

5.20 CNSI Meetings and Symposia

5.20.1. General

Any meeting (conference, seminar, exhibit) or symposium sponsored by NASA or held at a Center or NASA Headquarters where classified information is disclosed must meet the minimum-security standards established in paragraph 5.20.3. Meetings held by an association, society, or other group whose membership consists of primarily cleared contractors may be sponsored by NASA, provided an appropriately cleared contractor is designated and accepts responsibility for furnishing all symposium security measures.

5.20.2. Responsibilities

5.20.2.1. Key officials of the Office of the Administrator, Officials-In-Charge of Headquarters Offices, and Center Directors, as appropriate, are responsible for ensuring that AA/OSPP approval is obtained for a NASA-sponsored conference or symposium involving CNSI discussion and presentations. Security approval shall be coordinated with the Office of External Relations regarding the attendance of any foreign nationals or representatives at a CNSI symposium or meeting.

5.20.2.2. The CCS is responsible for ensuring that all minimum-security standards are met.

5.20.3. Minimum Standards

5.20.3.1. A CNSI meeting or symposium shall be restricted to appropriate areas at Government facilities approved for CNSI discussions or appropriate cleared contractor facilities.

5.20.3.2. Supervisors and meeting hosts shall ensure that all attendees possess the appropriate personnel security clearances and a **need-to-know** .

5.20.3.3. A request for security approval for a CNSI symposium shall be forwarded through the CCS to the DSMD and shall include the following items: date(s) and specific location for the proposed meeting (Government or cleared contractor facility), identification of CNSI subject matter and highest classification level involved, and the identification and status of any non-U.S. citizen (Foreign National or resident alien) and foreign representative invited to attend during any classified or unclassified session.

5.20.3.4. If any non-U.S. citizen, foreign national (to include resident aliens), or foreign representative shall be in attendance, the following information must be submitted to the DSMD: complete name, date, and place of birth; current citizenship status; type of personnel security clearance, if any; identification of each foreign Government, firm, and/or entity represented; date(s) of attendance; nature of participation, and the reason why attendance is considered to be in the U.S. national interest.

5.20.3.5. Foreign nationals or representatives shall not be extended an invitation to attend or be permitted to attend any CNSI or unclassified session unless advance approval has been obtained from the DSMD. Refer to NPR 1371.2A, Procedural Requirements for Processing Requests for Access to NASA Installations or U.S. Citizens who are Representatives of Foreign Entities, for more detailed requirements on facilitating Foreign National visits.

5.21 Security Container, Vault, and Strong Room Management

5.21.1. Deployment, use, and maintenance of security containers, vaults, or strong rooms designed for storage of CNSI shall be centrally managed by the CCS to ensure their use is consistent with Agency and Center policies and procedures for storage and accountability of CNSI. The CCS shall:

5.21.1.1. Ensure only GSA-approved security containers, designed specifically for storage of CNSI, are used. (NOTE: File containers with lock-bar are not authorized for the storage of TOP Secret material. Lock-bar containers must be completely eliminated from the Center inventory of authorized CNSI storage media NLT December 31, 2005.)

5.21.1.2. Maintain a current database of all Centerwide security containers, vaults, and strong rooms to include, at a minimum:

a. Assigned Center-specific security container, vault, or strong room number (e.g., ARC 000465).

b. Location of container, vault, or strong room (building/room#).

c. Custodian/Alternate custodian.

d. Highest classification level of information stored.

5.21.1.3. Ensure approved containers, vaults, and strong rooms are used only for storage of CNSI and necessary unclassified reference materials. Storage of unclassified

materials must be kept to the absolute minimum.

5.21.1.4. Ensure high value items that are targets of theft such as funds, weapons, and precious metal are not to be stored in the same drawer as classified materials.

5.21.1.5. Ensure approved security containers, vaults, and strong rooms are appropriately decertified and properly tagged "Not for Storage of Classified Material" by the CCS prior for use in storage of non-classified material.

5.21.1.6. Establish procedures to remove unneeded security containers are removed from service and retain for future use or properly disposed.

5.21.1.7. Ensure locking mechanisms are properly outfitted with or upgraded to appropriate federally mandated 'X' series locks under the following circumstances:

a. When the security container, vault, or strong room is newly procured or reentered into service.

(NOTE: For storage of classified material: containers, vaults and strong rooms must be inspected, reconditioned as necessary, recertified, and designated in writing by the Center Locksmith and acknowledged by the CCS prior to being reentered into service.)

b. When the locking system requires replacement.

c. When, at the discretion of the CCS, funding is available to retrofit existing container or vault inventory, or

d. When the contain , er, vault or strong r , oom is used to store Top Secret, COMSEC, Special Access Required, or SCI information and material.

5.22 Classified Material is NOT Personal Property

5.22.1. Classified information is always official U.S. Government information and never personal property . Confusion sometimes arises about classified notes from a training course or conference. As classified material, it is official information that must be safeguarded, transmitted, and destroyed in accordance with this NPR. Classified notes cannot be removed from a NASA installation without the approval of the Center Director or CCS. Classified notes shall not be considered as working papers but as official information for which the Center/facility is responsible. It must be transmitted by one of the means authorized for transmittal of classified material and eventually destroyed by authorized means. When an individual leaves one NASA installation and transfers to another, the installation may officially transfer his/her notes classified material to the new NASA installation where the material shall again be available for his/her use. If the individual desires to have the material transferred to another U.S. Government agency, the CCS, as approved by the Center Director, may facilitate such transfers.

5.22.2. CNSI and SBU are always the property of the United States Government. Individuals who remove SBU or CNSI may be subject to disciplinary action up to and including prosecution under Title 18 and Title 50 USC and other applicable laws.

5.23 Security Classification Reviews for NASA Programs and Projects

5.23.1. Pursuant to NPR 7120.5B, 1.4.3.a.(b); 2.1.g.(3); 2.1.1.2; 2.1.1.3.k; et al.,

programs and projects must conduct formal security reviews that, in addition to personnel, physical, and information technology security, shall include reviews for traditional information classification security needs. Security reviews shall be undertaken to determine if information used or produced as part of a program or project, meets the requirements for designation as CNSI and/or Sensitive But Unclassified (SBU) controlled information. Project managers will:

a. Refer to Appendix O, "Mandatory Review Process for Determining Classification and/or Sensitivity Level of Information and Technology Process" Flow Chart for guidance in conducting the review, and;

b. Complete NASA Form 1733 **, "** Information and Technology Classification and/or Sensitivity Level Determination Checklist."

c. Include the Form 1733 as permanent program documentation and in any procurement related documentation.

5.23.2. Upon the conclusion of the security review, if the information surrounding or concerning the program of project, or portions thereof, meet one or more of the categories of information presented in the executive order, a Subject Matter Expert (SME) must develop an appropriate Security Classification Guide (SCG). The SME and project officials shall consider the level of classification needed for specific information. NOTE: See chapter 10 for a definition of an SME. There are three levels of classified national security information: Top Secret, Secret, and Confidential. Chapter 10 provides a definition of each. Subject matter experts (SME) must be able to specifically identify what particular information is under consideration for classification. The SME, weighing the information being protected against the definitions in chapter 10, shall provide a recommendation to the Office of Security and Program Protection (OSPP) as to what level the information must be classified (Top Secret, Secret or Confidential) and how long the information must be kept classified. Duration of classification shall be considered within the following guidelines:

a. The SME shall attempt to determine a date or event that is less than 10 years from the date of original classification and which coincides with the lapse of the information's national security sensitivity and shall assign such date or event as the declassification instruction.

b. If unable to determine a date or event of less than 10 years, the SME shall ordinarily assign a declassification date that is 10 years from the date of the original classification decision.

c. If unable to determine a date or event of 10 years, the SME shall assign the declassification date not to exceed 25 years from the date of the original classification decision.

5.23.2.1. All SCGs must be approved by the OSPP. The DSMD shall assist program and project managers in the development of SCGs.

5.23.2.2. The OSPP will establish and maintain a central repository for all NASA originated SCGs and declassification guides, and shall provide a sequential numbering schema for all SCGs and declassification guides both classified and unclassified. The OSPP will also obtain and maintain SCGs and declassification guides from other agency programs in which NASA is working or supporting.

5.23.2.3. The SCG must be reviewed for updating every 5 years.

5.23.2.4. Upon completion, termination, or cancellation of a program or project, a declassification guide must be produced to provide the necessary requirements for declassifying the project information. The declassification guide must be approved by the OSPP.

5.23.2.5. The " *NASA Handbook for Writing Security Classification Guides* " provides requirements and guidance for the creation of a SCG.

5.23.3. If information surrounding or concerning the program or project is considered to be unclassified, a letter of transmittal shall be produced that reflects this determination. The original letter shall be maintained by the Project Office, with copies sent to the Mission Directorate Office having responsibility for the project or Center and to the DSMD.

5.23.4. If information surrounding or concerning the program or project is considered to be SBU, the information shall be managed as prescribed in section 5.24 of this NPR.

5.23.5. All CNSI and SBU information should be reviewed by a Record Manager, the responsible Program Manager or head of the office and a Declassification Authority (DCA), if the information is classified, to determine the disposition of the records before they are sent to the Federal Records Center (FRC) or the National Archives and Record Administration (NARA) for temporary or permanent storage.

5.24 Sensitive But Unclassified (SBU) Controlled Information

The Computer Security Act of 1987, Public Law 100-235, defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy."

5.24.1. With the exception of certain types of information protected by statute, standard criteria and terminology defining the types of information warranting designation as "sensitive information" does not exist within the Federal government. Such designations are left to the discretion of each individual agency. Therefore, NASA has determined that official information and material of a sensitive but unclassified (SBU) nature that does not contain national security information (and therefore cannot be classified) shall be protected against inappropriate disclosure by designating and handling such information as SBU in accordance with the procedures set forth in this NPR. See also the definition of Sensitive Information/Material in Chapter 10, "Glossary of Terms, Abbreviations, and Acronyms."

5.24.1.1. Information, regardless of its form (digital, hard-copy, magnetic tape, etc.), the release of which could cause harm to a person's privacy or welfare, adversely impact economic or industrial institutions, or compromise programs or operations essential to the safeguarding of our national interests is designated as SBU to control or restrict its access. Information designated as SBU shall be afforded appropriate protection sufficient to safeguard it from unauthorized disclosure.

5.24.1.2. Within NASA and the Federal Government, such information had previously been designated "FOR OFFICIAL USE ONLY." This designation was changed at NASA

to "Administratively Controlled Information" for clarity and to more accurately describe the status of information to be protected. However, recent efforts to apply consistent terminology across multiple federal agencies have prompted NASA to change the designation to "Sensitive but Unclassified." Therefore the caveat "SENSITIVE BUT UNCLASSIFIED (SBU)" will be used to identify sensitive but unclassified information within the NASA community when that information is not otherwise specifically described and governed by statute or regulation. The use of caveats other than SBU will be governed by the statutes and regulations issued for the applicable category of information.

5.24.1.3. The SBU designation and procedures set forth herein do not apply to the information, reports, or analysis by members of other agencies or departments who are members of the National Intelligence Board (NIB), who are on loan to NASA, and whose authorities are derived from other sources. However, SBU designation and procedures shall be applied when such information, or portions thereof, is copied for dissemination within NASA.

5.24.2. Identification of SBU Information. The failure to sufficiently identify information that requires protection from disclosure may result in increased risk to life or mission essential assets, damage to official relationships, monetary or other loss to individuals or firms, or embarrassment to NASA.

5.24.2.1. The originator of information, or the official approving its dissemination, must review the information for possible designation as SBU prior to its use. In general, information to be designated as SBU falls into one of the 3 categories described below. The criteria of at least one of the following subparagraphs must be met to designate the information as SBU:

a. Information originated within or furnished to NASA that falls under one or more of the exemption criteria of the Freedom of Information Act (5 U.S.C. §552). However, designating information as SBU does not represent that the information has been determined to be exempt from disclosure under FOIA. Requests under FOIA, for information designated as SBU, will be reviewed and processed in the same manner as any other FOIA request.

b. Information exempt or restricted from disclosure by statute, regulation, contract, or agreement. The following are examples of such information.

(1) Information subject to export control under the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR)

(2) Information disclosing a new invention in which the Federal Government owns or may own a right, title, or interest.

(3) Proprietary information of others provided to NASA under a nondisclosure or confidentiality agreement.

(4) Source selection and bid and proposal information.

(5) Small Business Innovative Research Data, Limited Rights Data, and Restricted Computer Software received in performance of NASA contracts.

(6) Information developed by NASA under a Space Act agreement and subject to section 303(b) of the Space Act (42 U.S.C. 2454(b)).

(7) Information concerning or relating to private entity trade secrets or confidential commercial or financial information received by a NASA employee in the course of government employment or official duties.

(8) Information subject to the Privacy Act of 1974 (5 U.S.C. §552a)

c. Information that is determined by a designated NASA official to be unusually sensitive (refer to paragraph 5.22.5. for decontrol provisions). The following are examples of such information.

(1) Predecisional materials such as national space policy not yet publicly released, pending reorganization plans, or sensitive travel itineraries

(2) Geological and geophysical information and data, including maps, concerning wells.

(3) Center maps and/or plain text documents describing locations/directions (e.g., latitude, longitude, depth, etc.) of underground utility conduits (e.g., sewers, gas, data, communications, etc.).

(4) Drawings and specifications that identify existing or proposed security measures for mission essential infrastructure designated assets or other key resources

(5) Mission specific security plans that identify protective measures and procedures for assets that are sensitive in nature but are not classified. (Example: Payloads that utilize special nuclear materials, payloads that contain certain animal experiments, and STS missions, as determined by the CCS, etc.)

(6) Emergency contingency or continuity of operations plans that provide detailed information regarding emergency response processes and procedures that, if publicized, could give a potential adversary vital information with which to thwart or compromise emergency response efforts.

(7) Sensitive scientific and technical information (STI) (See NPD 2200.1 and NPR 2200.2 for requirements for documentation, approval, and dissemination of NASA STI).

(8) Information that could result in physical risk to personnel.

(9) NASA information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models.

(10) Systems security data revealing the security posture of the system. For example, threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation.

(11) Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities, whether to persons, systems, or facilities, not otherwise eligible for classification under Executive Order 12958, as amended.

(12) Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security.

(13) Developing or current technology, the release of which could hinder the objectives of NASA, compromise a technological advantage or countermeasure, cause a denial of

service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.

5.24.2.2. Information identified in paragraphs a. and b. below that has designation and protection criteria established by other statutes, regulations, NASA directives, etc., shall be protected and marked in accordance with those applicable directives.

a. Information or material that may already have individual, officially designated identification, protection, or management requirements (e.g., FAR, FOUO, Export Control, FOIA, STI), and/or established markings on the sheet(s) will be controlled in accordance with their respective requirements. However, for the purpose of uniformity and consistency, physical protection and disclosure requirements established for the broader spectrum of SBU will still apply.

b. Information exempted from disclosure by treaty, statute (e.g., Export Administration Regulations (EAR), International Traffic in Arms Regulation (ITAR), and Section 303(b) of the Space Act), or other agreements.

5.24.2.3. Other government agencies and international organizations may use different terminology to identify sensitive information, such as "Limited Official Use (LOU)," and "Official Use Only (OUO)." In most instances the safeguarding requirements for this type of information are equivalent to SBU. However, other agencies and international organizations may have additional requirements concerning the safeguarding of sensitive information. Follow the safeguarding guidance provided by the other agency or organization. Should there be no such guidance, the information will be safeguarded in accordance with the requirements for SBU as provided in this document. Should the additional guidance be less restrictive than in this document, the information will be safeguarded in accordance with this NPR.

5.24.2.4. Information shall not be marked or designated as SBU if it does not meet the criteria in paragraph 5.24.2.1.

5.24.2.5. New material derived from documents marked SBU shall carry forward the control marking, if any, from the source documents.

5.24.3. Marking for SBU

Information designated as SBU will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of SBU markings on information known by the holder to be SBU does not relieve the holder from safeguarding responsibilities. Where the SBU marking is not present on information known by the holder to be SBU, the holder of the information will protect it as SBU. Information protected by statute or regulation will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with such guidance need not be additionally marked SBU. If there is no specific guidance or marking requirements, information designated SBU will be marked as follows:

a. Prominently mark the top and bottom of the front cover, first page, title page, back cover and each individual page containing SBU information with the caveat "SENSITIVE BUT UNCLASSIFIED (SBU)."

b. Materials containing specific types of SBU information may be further marked with the applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE," in order to alert the reader of the type of information conveyed. Where the sensitivity of the information warrants additional access and dissemination restrictions, the originator may cite additional

access and dissemination restrictions. For example:

WARNING: *This document is SENSITIVE BUT UNCLASSIFIED (SBU) . It is to be controlled, stored, handled, transmitted, distributed, and disposed* of *in accordance with NASA policy relating to SBU information. This information shall not be distributed beyond the original addressees without prior authorization* of *the originator.*

c. SBU information being transmitted to recipients outside of NASA, for example, other federal agencies, state or local officials, NASA contractors, etc., shall include the following additional notice:

WARNING: *This document is SENSITIVE BUT UNCLASSIFIED (SBU) . It contains information that may be exempt from public release under the Freedom of Information Act* (5 *U.S.C.* 552) or other applicable laws or restricted from disclosure based on NASA policy. *It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with NASA policy relating to SBU information and is not to be released to the public or other personnel who do not have* a *valid "need-to-know" without prior approval of an authorized NASA official (see NPR 1600.1).*

d. Computer storage media, i.e., disks, tapes, removable drives, memory sticks, etc. containing SBU information will be marked "SENSITIVE BUT UNCLASSIFIED."

e. Portions of a classified document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only SBU information will be marked with the abbreviation (SBU).

f. Individual portion markings on a document that contains no other designation are not required.

5.24.4. Responsibilities.

5.24.4.1 Officers and employees designating information or materials as SBU and those receiving materials so marked shall be responsible for properly safeguarding the information contained therein. These individuals will:

a. Comply with the safeguarding requirements for SBU information as outlined in this document.

b. Participate in formal classroom or computer based training sessions presented to communicate the requirements for safeguarding SBU and other sensitive information and the penalties that could result in unauthorized disclosure of SBU information.

c. Keep the number of copies of SBU information to a minimum.

d. Require that all individuals performing work for NASA (contractors, consultants and other persons not employed directly by NASA) execute a NASA Form (TBD), "Sensitive But Unclassified Information Non- Disclosure Agreement (NDA)," as a condition of access to SBU information. Other individuals not assigned to, employed by or performing work for NASA, but to whom access to SBU information will be granted, may be required to execute an NDA as determined by the applicable program manager. Execution of the NDA shall be effective upon publication of this directive and not applied retroactively.

5.24.4.2. Supervisors and managers will:

a. Ensure that an adequate level of education and awareness is established and maintained to emphasize safeguarding and preventing unauthorized disclosure of SBU

information.

b. Ensure that an adequate level of education and awareness is established and maintained to emphasize that disclosing SBU information without proper authority could result in administrative or disciplinary action, fines and/or imprisonment.

c. Take appropriate corrective actions, to include administrative or disciplinary action as appropriate, when unauthorized disclosures of SBU information occur.

5.24.5. Decontrol Provisions. Officers and employees designating information or materials as SBU shall be held responsible for their continued review and the prompt removal of such designations and restrictive markings when the necessity no longer exists. Authority to decontrol such material and any copies is limited to the official who initially designated the material as SBU, a successor or superior, or an official of an office having primary interest in the material. The following procedures apply:

5.24.5.1. The control status of any information or material designated as SBUshall be reviewed upon request by an individual or individuals to whom disclosure has been restricted. Such material shall be decontrolled and disclosed unless the office of origin or the office of primary interest determines, within a reasonable period of time after the request and after consultation with legal counsel, that the information must remain protected against disclosure. The existence of an SBU marking does not necessarily make information exempt from disclosure. A determination that information is exempt from disclosure must be based on the applicability of some legal authority. Consultation with the Office of the General Counsel at Headquarters or Center Office of Chief Counsel is required.

5.24.5.2. The restrictive marking on information designated as SBU in accordance with paragraph 5.24.2.1. shall be immediately removed when the need for protection no longer exists, (e.g., imminent public release, transfer to records archives, implementation of organization plan, or conclusion of sensitive travel).

5.24.6. Storage, Access, Disclosure, Protection, Transmittal, and Destruction of SBU. The minimum requirements for storage, access, protection, transmittal, and destruction of SBU information is provided in section 5.24.6.1 through 5.24.6.5, respectively. However, some types of SBU information may be more sensitive than others and thus warrant additional safeguarding measures beyond the minimum requirements established in this NPR. For example, certain types of information may be considered extremely sensitive based on the consequences of an unauthorized release. Such consequences could be increased risk to life or mission essential assets, damage to official relationships, or embarrassment to NASA. Additional control requirements may be added as necessary to afford appropriate protection to such information. NASA employees, contractors, and detailees must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property as the basis for determining the need for safeguards in excess of the minimum requirements and protect the information accordingly.

5.24.6.1. Storage. Employees who handle information or material designated SBU shall ensure the proper safeguarding of such information by limiting its access to authorized persons only and by storing it in cabinets, desks, or other containers, or securing it within an individual office area when not in use. Access to SBU information is on a "need to Know" basis in accordance with section 5.24.6.2.

a. When unattended, SBU information will, at a minimum, be stored in a locked file

cabinet, locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza, or similar locked compartment. SBU information can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room, or an area where access is controlled by a guard, cipher lock, or card reader.

b. SBU information will not be stored in the same container used for the storage of classified information unless there is a correlation between the information. When SBU information is stored in the same container used for the storage of classified materials, they will be segregated from the classified materials to the extent possible, i.e. separate folders, separate drawers, etc.

c. IT systems that store SBU information will be certified and accredited for operation in accordance with federal and NASA standards. Consult the NPR 2810.1, Security Information Technology, for more detailed information.

d. Laptop computers and other media containing SBU information will be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure. Storage and control will be in accordance with NPR 2810.1.

5.24.6.2. Access and Disclosure. SBU information of which NASA or a NASA contractor is the originator may disclosed to any Federal Government employee or contractor who has a demonstrated "need-to-know" in connection with official duties. When NASA is not the originating agency, SBU information may be disclosed only with authorization from the originating or designated action agency. Whenever SBU information is disclosed, the recipient must be made aware of the following restrictions on access and disclosure:

a. In no case shall SBU information be disclosed - orally, visually, or electronically - unless the disclosure is clearly in accordance with existing law and Agency regulations or policy directives and is in the best interest of NASA.

b. Access to SBU information is based on "need-to-know" as determined by the holder of the information. When discussing with or transferring SBU information to another individual(s), the holder of the information must ensure that the individual with whom the discussion is to be held or the information is to be transferred has a valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, or from observing or otherwise obtaining the information. Where there is uncertainty as to a person's need-to-know, the holder of the information will request dissemination instructions from his/her next-level supervisor or the information's originator.

c. A security clearance is not required for access to SBU information.

d. SBU information may be shared with other agencies, federal, state, tribal, or local government and law enforcement officials, provided a specific need-to-know has been established and the information is shared in furtherance of a coordinated and official governmental activity. Where SBU information is requested by an official of another agency and there is no coordinated or other official governmental activity, a written request will be made from the requesting agency to the applicable NASA program office providing the name(s) of personnel for whom access is requested, the specific information to which access is requested, and basis for need-to-know. The NASA program office shall then determine if it is appropriate to release the information to the other a , gency official. (See section 5.24.3 for marking requirements)

e. When NASA is not the originating agency, further dissemination of SBU information by the holder of the information may be made only with authorization from the originating or designated action agency. When information requested or to be discussed originated with another agency, the holder of the information must comply with that originating agency's policy concerning third party discussion and dissemination.

,

f. The holder of the SBU information will comply with any access and dissemination restrictions cited on the material, provided with the material, or verbally communicated by the originator. Sensitive information protected by statute or regulation, i.e., Privacy Act, Critical Infrastructure Information, etc., will be controlled and disseminated in accordance with applicable guidance for that type of information. Where no guidance is provided, handle SBU information in accordance with the requirements of this NPR

g. NASA IT Systems containing SBU shall be appropriately protected from unauthorized access. Access shall be granted only after the requisite security investigation, as outlined in chapters 3 or 4 of this NPR, has been accomplished. In addition, access provisions for FIPS 199 Security Category Moderate shall apply.

h. When discussing SBU information over a telephone, the use of a STU III (Secure Telephone Unit), or Secure Telephone Equipment (STE), is encouraged, but not required.

5.24.6.3. Protection. When materials marked SBU are prepared for dissemination or forwarded to any locations/persons (within or outside a NASA Center), they must be protected using NASA Form 1686, "SENSITIVE BUT UNCLASSIFIED" (SBU) cover sheet. Users shall check appropriate boxes on the form to signify what type of SBU information is contained in the document.

a. When removed from an authorized storage location and persons without a need-to-know are present, or where casual observation would reveal SBU information to unauthorized persons, a SBU cover sheet (NASA Form 1686) will be used to prevent unauthorized or inadvertent disclosure.

b. When disclosing, disseminating, or transmitting SBU information, a SBU cover sheet, (NASA Form 1686), should be placed on top of the transmittal letter, memorandum, or material.

c. When receiving SBU equivalent information from another government agency, handle in accordance with the guidance provided by the other government agency. Where no guidance is provided, handle in accordance with the requirements of this NPR.

5.24.6.4. Transmittal. Transmission of SBU information may be made via first class mail, courier, encrypted e-mail, encrypted FTP, encrypted HTTP, or secure fax to known recipients. All transmissions of SBU information require a SBU cover sheet (NASA Form 1686) be transmitted with the information. Additionally, the holder of the SBU information will comply with any access, dissemination, and transmittal restrictions cited on the material, provided with the material, or verbally communicated by the originator.

a. Transmission of hard copy SBU information within the U.S. and its Territories:

(1) Material containing SBU information will be placed in a single opaque envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of

tampering. The envelope or container will bear the complete name and address of the sender and addressee, to include program office and the name of the intended recipient (if known).

(2) Material containing SBU information may be mailed by U.S. Postal Service First Class Mail or an accountable commercial delivery service such as Federal Express or United Parcel Service.

(3) Material containing SBU information may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.

b. Transmission of hard copy SBU information to Overseas Offices: When an overseas office is serviced by a military postal facility, i.e., APO/FPO, SBU may be transmitted directly to the office. Where the overseas office is not serviced by a military postal facility, the SBU information will be sent through the Department of State, Diplomatic Courier.

c. Electronic Transmission.

(1) Transmittal via fax. The use of a secure fax machine is highly encouraged. However, unless otherwise restricted by the originator, SBU information may be sent via nonsecure fax. Where a nonsecure fax is used, the sender will coordinate with the recipient to ensure that the SBU information faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end.

(2) Transmittal via E-Mail, FTP, and HTTP (Web)

(i) SBU information transmitted via email, FTP, web, etc., should be protected by encryption or transmitted within secure communications systems. If it is not possible to transmit SBU via appropriately encrypted channels, the information can be included as a password protected attachment with the password provided under separate cover. Recipients of SBU information will comply with any email or other electronic transmission restrictions imposed by the originator.

(ii) Due to inherent vulnerabilities, SBU information shall not be sent to personal email accounts.

(3) NASA Internet/Intranet

(i) SBU information will not be posted on a public NASA website or any other public website.

(ii) SBU information may be posted on the NASA Intranet or other government controlled or sponsored protected encrypted data networks. However, the official authorized to post the information should be aware that access to the information is open to all personnel who have been granted access to that particular Intranet site. The official must determine the nature of the information is such that need-to-know applies to all such personnel; the benefits of posting the information outweigh the risk of potential compromise; the information posted is prominently marked as SENSITIVE BUT UNCLASSIFIED; and information posted does not violate any provisions of the Privacy Act or other applicable laws.

5.24.6.5. Destruction. SBU information or material that cannot be decontrolled per paragraph 5.24.5 or which is no longer needed shall be removed from IT systems,

shredded, burned, or destroyed in other similar methods that preclude unauthorized disclosure. Destruction may be accomplished by:

a. "Hard Copy" materials will be destroyed by shredding, burning, pulping, pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.

b. Electronic storage media shall be sanitized appropriately by overwriting or degaussing, or non-recoverable encrypted deletion. Contact local IT security personnel for additional guidance.

c. Paper products containing SBU information will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

5.24.6.6. Disposal of IT Systems Containing SBU. Refer to NPR 2810.1 for procedural requirements regarding clearing of hard drives, blackberries, personal digital assistant (PDA's), and other storage mediums, prior to disposal or recycling.

5.24.7. Incident Reporting. The loss, compromise, suspected compromise, or unauthorized disclosure of SBU information will be reported. Incidents involving SBU in NASA IT systems will be reported to the center IT Security Manager in accordance with IT incident reporting requirements in NPR 2810.1.

5.24.7.1. Suspicious or inappropriate requests for information by any means, e.g., email or verbal, shall be report to the NASA Center Chief of Security.

5.24.7.2. Employees or contractors who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of SBU information will report it immediately, but not later than the next duty day, to the originator and the Center Chief of Security.

5.24.7.3. Additional notifications to appropriate NASA management personnel will be made without delay when the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned or on-going operation.

5.24.7.4. At the request of the originator, an inquiry will be conducted by the center security official or other designee to determine the cause and affect of the incident and the appropriateness of administrative or disciplinary action against the offender

5.24.8. Administrative Violations and Sanctions.

5.24.8.1. All NASA employees, as well as non-employees, who have access to SBU are responsible individually for complying with the provisions of this NPR and may be subject to administrative sanctions if they disclose information designated SBU without proper authorization.

5.24.8.2. Sanctions include, but are not limited to warning notice, admonition, reprimand, suspension without pay, forfeiture of pay, removal, and/or discharge.

5.24.8.3. Such sanctions may be imposed, as appropriate, upon any person determined to be responsible for a violation of disclosure restrictions in accordance with applicable law and regulations, regardless of office or level of employment.

5.25 Use, Protection, and Accountability of Department of Energy (DoE) Unclassified Controlled Nuclear Information (UCNI)

5.25.1. Use.

5.25.1.1. UCNI is sensitive unclassified Government information concerning nuclear material, weapons, and components, whose dissemination is controlled under section 148 of the Atomic Energy Act.

5.25.1.2. It is to be accessed only by personnel with a need-to-know.

5.25.1.3. Foreign Nationals are not authorized access without approval of DoE.

5.25.2. Protection.

5.25.2.1. UNCI must be stored to prevent unauthorized disclosure. Securing in a locked room, file cabinet, or desk drawer is the minimum requirement.

5.25.2.2. UCNI may be reproduced.

5.25.2.3. Use of encryption is mandatory for electronic transmission.

5.25.2.4. Use of a Secure Telephone Unit (STU III) or Secure Telephone Equipment (STE) is mandatory whenever conversations involving UCNI are necessary.

5.25.3. Accountability.

5.25.3.1. Organizations using UCNI shall designate in writing a Reviewing Official responsible for reviewing created NASA correspondence, reports, and related materials for the presence of UCNI and ensuring the appropriate marking per DoE policy.

5.25.3.2. All copies of UCNI must be periodically inventoried to ensure appropriate accountability.

5.25.3.3. Unneeded copies shall be destroyed by burning or shredding.

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

| NODIS Library | Organization and Administration(1000s) | Search |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.
Check the NASA Online Directives Information System (NODIS) Library

to Verify that this is the correct version before use: http://nodis3.gsfc.nasa.gov